

MAR 26 2019

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF ARKANSASJAMES W. McCORMACK, CLERK
By: [Signature] DEP CLERKWILLIAM BOYD, Individually and On
Behalf of All Others Similarly Situated,

Plaintiff,

v.

MARRIOTT INTERNATIONAL, INC.,
and STARWOOD HOTELS & RESORTS
WORLDWIDE LLC,

Defendants.

Case No. 4:19cv205-Saw

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

This case assigned to District Judge Wright
and to Magistrate Judge Harris

Plaintiff William Boyd ("Plaintiff") brings this class action on behalf of himself and all others similarly situated, by and through undersigned counsel, and for his complaint against Marriott International, Inc. ("Marriott") and Starwood Hotels & Resorts Worldwide LLC ("Starwood") (referred to collectively as "Defendants"), states and alleges, upon personal knowledge as to himself and otherwise upon information and belief, as follows:

INTRODUCTION

1. This action arises from a *four-year* long data breach experienced by Defendants wherein the data of over 500 million customers of Marriott's Starwood division was compromised (the "Marriott Data Breach"). Due to the extraordinary quantity of data leaked over this four-year time span, the Marriott Data Breach is being heralded as not only the largest data breach of 2018, but also as the second largest data breach of all time.

2. On November 30, 2018, Marriott—the world's largest hotel chain—announced that on September 8, 2018, it learned of an unauthorized access to its Starwood guest reservation database. Upon investigation thereof, Marriott learned that the breach had allowed hackers to access its customer data starting as early as *2014* and extending through September 10, 2018.

3. Marriott further revealed that the Marriott Data Breach allowed unauthorized access to guest information relating to reservations at Starwood properties that affected at least 500 million people. For at least 327 million of these guests, the information includes, but is not limited to, guests' "name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communications preferences."¹

4. Marriott disclosed that for some affected guests, the siphoned data included payment card information, including payment card numbers and expiration dates ("Payment Card Information"), and while this information was encrypted, Marriott could *not* rule out the possibility that hackers obtained the encryption keys necessary to decrypt and access this data.²

5. Defendants' laxity and security deficiencies were so significant that hackers were not only able to breach Defendants' systems, but they were able to go undetected for a four-year time period. As one privacy expert stated, "They can say all they want that they take security seriously, but they don't if you can be hacked over a four-year period without noticing."³

6. Defendants' security failures put Plaintiff's and Class and Subclass members' (defined below) personal information at serious, immediate, and ongoing risk, resulting in costs and expenses to Plaintiff and members of the Class and Subclass in time spent and the loss of productivity in taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the theft of their personal information.

¹ *Marriott Announces Starwood Guest Reservation Database Security Incident*, <http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/> (last visited Mar. 26, 2019).

² *Id.*

³ Nicole Perlroth, et al., *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. TIMES (Nov. 30, 2018), <https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html> (last visited Mar. 26, 2019).

7. The Marriott Data Breach was caused and enabled by Marriott's failure to implement and maintain reasonable and adequate security measures and protocols, consistent with the representations Marriott made to the public in its marketing materials and privacy statements, and compliant with industry standards, best practices, and the requirements of applicable law.

8. In point of fact, in November 2015, Starwood reported a security breach when it detected malware on its point of sale ("POS") systems in over 100 locations in North America. Upon investigation of the incident, which occurred from November 2015 through January 2016, Marriott incorrectly assessed that the Starwood customer reservation database—the database at issue in the Marriott Data Breach—had not been impacted. The investigation should have revealed the Marriott Data Breach.⁴

9. Plaintiff is a Marriott customer who brings this proposed class action individually and on behalf of all persons who have suffered, and continue to suffer, financial losses and increased data security risks arising as a direct result of Defendants' failure to safeguard their personal information. This information includes, but is not limited to, names, phone numbers, passport numbers, date of birth, gender, mailing and email addresses, arrival and departure information, and Payment Card Information (collectively referred to as "PII").

10. Plaintiff and the Classes have incurred, and will continue to incur, substantial costs in taking measures to protect their PII in addition to monitoring for identity theft.

11. Plaintiff seeks to recover the costs incurred as a result of Defendants' data breach and to obtain appropriate declaratory and injunctive relief to mitigate future harm.

⁴ Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, WSJ (Dec. 2, 2018), <https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659> (last visited Mar. 26, 2019).

PARTIES

12. Plaintiff William Boyd is a citizen of Pulaski County, Arkansas. Plaintiff provided Defendants with his PII, and, as a result of Defendants' actions, Plaintiff has suffered financial losses and will face a substantial risk for further identity theft.

13. Defendant Marriott International, Inc. ("Marriott") is a publicly-traded corporation with its principal place of business at 10400 Fernwood Road, Bethesda, Maryland 20817.

14. Defendant Starwood Hotels & Resorts Worldwide, LLC ("Starwood") is an indirect, wholly-owned subsidiary of Marriott. On September 23, 2016, Marriott completed the acquisition of Starwood Hotels & Resorts Worldwide, LLC, formerly known as Starwood Hotels & Resorts Worldwide, Inc.

JURISDICTION AND VENUE

15. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed \$5,000,000 exclusive of interests and costs; there are more than 100 putative class members; and minimal diversity exists because the majority of putative class members are citizens of a different state than Defendants.

16. This Court has personal jurisdiction over Defendants because they reside in this District and regularly conduct business here. Upon information and belief, a substantial portion of the events and conduct giving rise to this litigation occurred in this District.

17. This District is the proper venue because a substantial portion of the injury from Defendants' conduct occurred in this District.

FACTUAL ALLEGATIONS

A. Defendants Collect and Store Guest Information

18. With 6,500 properties in 127 countries and over \$20 billion in revenue in 2017, Marriott is the largest hotel chain in the world.

19. The acquisition of Starwood by Marriott was announced on November 16, 2015 and finalized on September 23, 2016. Through the acquisition, Marriott came to control the rights to the Starwood properties.

20. Starwood collects a substantial amount of PII, including Payment Card Information, from guests looking to stay at one of the Starwood Properties. This information is generally not destroyed but is stored in the Reservation Database.⁵

21. Marriott has admitted that the information contained in the Reservation Database includes some combination of name, mailing address, phone number, email address, passport number, account information, date of birth, gender, stay information, and communication preferences for over 300 million guests, along with Payment Card Information for additional guests.⁶

22. Marriott first learned on September 8, 2018 that an attempt was made to access the Reservation Database.⁷ It was only upon further investigation that Marriott learned hackers had first gained access to the Reservation Database in 2014 and had copied, encrypted, and attempted to remove the PII, including the Payment Card Information.⁸

⁵ *Starwood Guest Reservation Database Security Incident*, Nov. 30, 2018, <https://answers.kroll.com/> (last visited Mar. 26, 2019).

⁶ *Marriott says its Starwood database was hacked for approximately 500 million guests*, CNBC (Nov. 30, 2018), <https://www.cnbc.com/2018/11/30/marriott-says-its-starwood-database-was-breached-onapproximately-500-million-guests-.html> (last visited Mar. 26, 2019).

⁷ *Starwood Guest Reservation Database Security Incident*, Nov. 30, 2018, <https://answers.kroll.com/> (last visited Mar. 26, 2019).

⁸ *Id.*

23. Investigators have stated that “multiple hacking groups may have simultaneously been inside Starwood’s computer networks since 2014.”⁹ The fact that multiple groups were able to infest the Reservation Database over the same period shows that Marriott failed to adequately safeguard its guests’ information.

B. The Risk of a Breach was Foreseeable

24. Defendants should have been aware that the guest information it was collecting made a tempting target for criminals.

25. The Reservation Database information is valuable for hackers because includes guest’s biographical data and “[i]ncreasingly, criminals are using biographical data gained from multiple sources to perpetrate more and larger thefts.”¹⁰ Thieves can use large data pools like the Reservation Database as a tool to commit further acts of identity theft or create new identities from a merger of separate biographical details.

26. This is not a theoretical problem, as the hotel industry has a history of being targeted by hackers.

27. Before being acquired by Marriott in 2015, Starwood was aware of a malware intrusion that affected its hotels in North America, enabling hackers to access the Payment Card Information of some guests.¹¹

28. In June 2017, cybersecurity researchers discovered in an ironic twist that Marriott’s Computer Incident Response team was compromised by “Russian criminals to run a

⁹ *Exclusive: Clues in Marriott hack implicate China*, Reuters (Dec. 5, 2018), <https://uk.reuters.com/article/uk-marriott-intnl-cyber-china/clues-in-marriott-hack-implicate-china-sources-idUKKBN1O504B> (last visited Mar. 26, 2019).

¹⁰ Verizon 2014 PCI Compliance Report, http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf, at 54 (last visited Mar. 26, 2019).

¹¹ Starwood Hotels and Resorts, Letter from our President (Nov. 20, 2015), https://oag.ca.gov/system/files/starwood-notice-materials_0.pdf (last visited Mar. 26, 2019).

network of hacked servers.”¹²

29. These incidents have not been confined to Marriott properties.

30. In 2008 and 2009, over 619,000 Wyndham accounts were obtained by hackers.¹³

The FTC settled with Wyndham, requiring Wyndham to undergo substantial monitoring for 20 years.¹⁴

31. On March 17, 2015, the Mandarin Oriental announced that its credit card systems had been compromised by hackers.¹⁵

32. On October 31, 2017, it was reported that Hilton Hotels agreed to pay \$700,000 as part of a settlement with the New York and Vermont Attorneys General arising out of data breaches that exposed over 350,000 credit card numbers.¹⁶

33. In light of these industrywide hacks, Defendants were on notice that their databases were a likely target for hacking and should have taken care and ensured that proper data security systems were in place. However, they did not.

¹² Thomas Brewster, *Revealed: Marriott's 500 Million Hack Came After A String of Security Breaches*, Forbes (Dec. 3, 2018), <https://www.forbes.com/sites/thomasbrewster/2018/12/03/revealed-marriotts-500-million-hack-came-after-a-string-of-security-breaches/#3dba0b9546f4> (last visited Mar. 26, 2019).

¹³ Sean O'Neill, *Marriott's Starwood Data Breach Joins a Decade-Long List of Hotel Data Exposures*, Skift (Nov. 30, 2018), <https://skift.com/2018/11/30/marriotts-starwood-data-breach-joins-a-decade-long-list-of-hotel-data-exposures/> (last visited Mar. 26, 2019).

¹⁴ Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk (Dec. 9, 2015), <https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment> (last visited Mar. 26, 2019).

¹⁵ Credit Card Breach at Mandarin Oriental (Mar. 4, 2015), <https://krebsonsecurity.com/2015/03/credit-card-breach-at-mandarian-oriental/> (last visited Mar. 26, 2019).

¹⁶ Jonathan Stempel, *Hilton to Pay \$700,000 Over Credit Card Data Breaches*, Reuters (Oct. 31, 2017), <https://www.reuters.com/article/us-hilton-wrldwide-settlement/hilton-to-pay-700000-over-credit-card-data-breaches-idUSKBN1D02L3> (last visited Mar. 26, 2019).

C. Defendants Failed to Comply with Government & Industry Standards

34. According to the FTC, the failure to employ reasonable and appropriate measures to guard against unauthorized access to confidential consumer data constitutes an unfair practice or act prohibited by Section 5 of the Federal Trade Commission Act of 1914 (“FTC Act”), 15 U.S.C. § 45.

35. The FTC has published guidelines for businesses that establish reasonable data security practices. The practices center around knowing what personal information is stored, keeping only what information is absolutely necessary, securely guarding the information that is kept, disposing of the information that is not needed, and having a plan in place to respond to security incidents.¹⁷

36. The FTC has also published a guidance handbook on data security practices for businesses based on its past enforcement actions.¹⁸ This provides further guidance into what data security practices are expected from businesses that handle personal information.

37. The Payment Card Industry Security Standards Council promulgates a set of minimum requirements that apply to all organizations that store, transmit, or process Payment Card Information. This standard is known as the Payment Card Industry Data Security Standard (“PCI DSS”) and is the bare-minimum industry standard governing Payment Card Information security.

38. PCI DSS required Defendants to properly secure Payment Card Information, restrict access to Payment Card Information on a need-to-know basis, encrypt Payment Card

¹⁷ See Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business> (last visited Mar. 26, 2019).

¹⁸ See Federal Trade Commission, *Start with Security: A Guide for Business; Lessons Learned from FTC Cases*, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited Mar. 26, 2019).

Information at the time of entry, implement network segmentation, only hold Payment Card Information for the time required to verify a transaction, and establish processes to identify and fix data vulnerabilities.

39. As discussed throughout, Defendants failed to comply with both government and industry standards.

D. Marriott's Delayed Response Exacerbated the Situation

40. Marriott first stated that it had received an alert regarding an attempt to access the Reservation Database on September 8, 2018.¹⁹

41. Over a month later on November 19, 2018, Marriott announced that was able to decrypt the hacked information and determined that it originated from the Reservation Database.²⁰

42. Despite the severity of the breach and the nature of the stolen information, Marriott waited an additional eleven (11) days to inform the public of the breach.

43. In response to its abject failure to protect and safeguard its guests' PII, Marriott has offered only a year of identity-theft protection and to pay for replacement passports if guests can prove that they are the victims of passport-related identity theft.²¹

44. This assumes that the risk of identity theft will only continue for a year and fails to appreciate that the risk of identity theft is immediate and ongoing. Guests need replacement documents immediately or they run the risk of having their identities stolen or manipulated.

¹⁹ *Starwood Guest Reservation Database Security Incident*, Nov. 30, 2018, <https://answers.kroll.com/> (last visited Mar. 26, 2019).

²⁰ *Id.*

²¹ Nicole Perlroth, et al., *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. TIMES (Nov. 30, 2018), <https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html> (last visited Mar. 26, 2019); Grace Dobush, *Starwood Data Hack: Marriott Says It'll Pay for New Passports*, FORTUNE (Dec. 4, 2018), <https://finance.yahoo.com/news/starwood-data-hack-marriott-says-122147510.html> (last visited Mar. 26, 2019).

45. Furthermore, Marriott failed to announce the data breach in a timely or professional manner.

46. Marriott stated that the process of emailing guests to notify them of the breach would take several weeks, far too long to communicate information of this magnitude.²²

47. The email that Marriott finally sent to affected guests came from the domain “email-marriott.com,” leading technology reports to state “there was little else to suggest the email was at all legitimate – the domain doesn’t load or have an identifying HTTPS certificate. In fact, there’s no easy way to check that the domain is real, except a buried note on Marriott’s data breach notification site that confirms the domain is legitimate.”²³ As a result of Marriott’s lackluster response and in order to prevent further harm to Marriott consumers, two security experts registered similarly named domains, email-marriot.com and email-mariott.com,²⁴ to prevent hackers from obtaining them.²⁵

E. Plaintiff and Members of the Classes Face Ongoing Harm Caused by the Marriott Data Breach

48. Defendants have failed to follow government and industry data protection standards and have failed to effectively monitor their own security systems to ensure guest information is protected.

²² Robert McMillan, *Marriott’s Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, WSJ (Dec. 2, 2018), <https://www.wsj.com/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659> (last visited Mar. 26, 2019).

²³ Zach Whittaker, *Marriott’s Breach Response is so Bad, Security Experts are Filling in the Gaps – At Their Own Expense*, TechCrunch (Dec. 3, 2018), <https://techcrunch.com/2018/12/03/marriott-data-breach-response-risk-phishing/> (last visited Mar. 26, 2019).

²⁴ To the untrained eye, these look like legitimate domains; however, both misspell “Marriott”.

²⁵ Zach Whittaker, *Marriott’s Breach Response is so Bad, Security Experts are Filling in the Gaps – At Their Own Expense*, TechCrunch (Dec. 3, 2018), <https://techcrunch.com/2018/12/03/marriott-data-breach-response-risk-phishing/> (last visited Mar. 26, 2019).

49. The substandard security system in place and the failure to adequately monitor that system for unauthorized intrusions caused Plaintiff and the Classes' PII, including Payment Card Information, to be compromised over a four-year period without detection by the Defendants.

50. Because of Defendants' failure to meet reasonable security standards, Plaintiff and members of the Classes have suffered, and will continue to suffer, substantial harm.

51. As a result of the Defendants' actions and the resulting data breach, Plaintiff and members of the Classes must cancel credit and debit cards, change or close their financial accounts, monitor credit reports for fraudulent activity, and take other steps to protect themselves in order to reduce the risk of identity theft and fraudulent transactions.

52. The information compromised in the Marriott Data Breach is a veritable treasure trove for criminals. Through that information, criminals now have access to a complete profile of guests' personal and financial information. They can either use this information themselves or sell it on the black market for others. Either way, criminals can now assume these stolen identities to apply for loans, open accounts, forge checks, file fraudulent tax returns, or forge government-issued documents.

53. This is not an abstract risk. The Department of Justice has reported that, for one year alone, 86% of identity theft victims experienced the fraudulent use of existing account information, including credit card and bank account information.²⁶

54. This risk is ongoing. The information obtained from this breach will be available to criminals on the web for an indefinite period. This means that Defendants' guests face an

²⁶ Erika Harrell, *Victims of Identity Theft, 2014*, U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS, NCJ 248991 (Sept. 2015) at 2, <https://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited Mar. 26, 2019).

ongoing harm that Defendants seem unwilling or unable to redress in any meaningful way.

CLASS ACTION ALLEGATIONS

55. Plaintiff brings this action on behalf of himself and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3) on behalf of the following:

National Class (the “Class”):

All individuals whose PII and/or Payment Card Information was accessed, copied, and/or compromised by unauthorized parties as part of the Marriott Data Breach.

Arkansas Subclass (the “Subclass”):

All Arkansas residents whose PII and/or Payment Card Information was accessed, copied, and/or compromised by unauthorized parties as part of the Marriott Data Breach.

(collectively the Class and Subclass are referred to as the “Classes”).

Rule 23(a)

56. This action may be maintained as a class action if it meets the requirements of Fed. R. Civ. P. 23(a): Numerosity, Commonality, Typicality, Adequacy.

57. **Numerosity.** The members of the Classes are so numerous that joinder of all parties would be impracticable. While Plaintiff does not know the exact number of the members of the Classes, Plaintiff believes the Class contains hundreds of millions of members, with tens of thousands of members in the Subclass.

58. **Commonality.** Common questions of law and fact predominate over individual questions and facts. These common questions include, but are not limited to:

- a. Whether Defendants owed a duty to Plaintiff and the Classes to protect PII and/or Payment Card Information;
- b. Whether Defendants failed to provide adequate security to protect PII and/or Payment Card Information;
- c. Whether Defendants negligently allowed PII and/or Payment Card

Information to be accessed by third parties;

- d. Whether Defendants failed to adequately notify Plaintiff and the Classes that data systems were breached;
- e. Whether Plaintiff and members of the Classes suffered damages;
- f. Whether Defendants' actions proximately caused the injuries suffered by Plaintiff and the Classes;
- g. Whether Plaintiff and the Classes are entitled to damages, and if so, the amount thereof; and
- h. Whether Plaintiff and the Classes are entitled to declaratory and injunctive relief.

59. **Typicality.** Plaintiff's claims are typical of the absent class members and stem from the same series of events. Plaintiff and members of the Classes are all persons injured by Defendants' data breach, and Plaintiff's claims arise from the same practices and course of conduct giving rise to the claims of the absent Class Members and are based on the same legal theories. The claims of each member of the Classes would rely on the same facts and legal theories and seek the same relief if prosecuted individually.

60. **Adequacy.** Plaintiff will fully and adequately represent the interests of the Classes. Plaintiff has retained Class counsel who have considerable experience in class action litigation. Neither Plaintiff nor his attorney has any interests that conflict with the interests of the Classes.

Rule 23(b)(3)

61. The questions of law and fact common to all members of the Classes predominate over any questions affecting only individuals.

62. A class action is superior to other available methods because the individual litigation of the absent class members' claims is economically infeasible and procedurally impracticable. Litigating the claims together will prevent varying, inconsistent, or contradictory judgments and preserve judicial resources and prevent delay and expense for all parties. Class treatment will also permit members of the Classes to litigate claims where it would otherwise be too expensive or inefficient to do so. Plaintiff knows of no difficulties in managing this action that would preclude its maintenance as a class action.

63. Contact information for each class member, including mailing addresses is readily available, facilitating notice of the pendency of this action.

Rule 23(b)(2)

64. Injunctive relief is appropriate because Defendants' inadequate security exposes all members of the Classes to a substantial risk of immediate harm. Injunctive relief is necessary to uniformly protect the Classes' data. Plaintiff seeks prospective injunctive relief as a separate remedy from any monetary relief.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Negligence

65. Plaintiff incorporates the above allegations as if fully set forth herein.

66. Defendants owed Plaintiff and the Classes a duty to exercise reasonable care in the collection, storage, and protection of their PII and Payment Card Information.

67. Defendants also assumed a duty to use reasonable care to implement a policy and process to prevent unauthorized access to the PII and Payment Card Information by third parties.

68. Defendants knew or should have known that by collecting and storing PII and Payment Card Information, they created a valuable target for third-party interference, targeting, or theft.

69. Defendants knew or should have known that their databases were vulnerable to unauthorized third-party access.

70. Once Defendants chose to collect and store PII and Payment Card Information belonging to Plaintiff and the Classes, only Defendants were in a position to guard that data repository from the foreseeable risk of third-party interference, targeting, or theft.

71. Defendants' duty also arose under Section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII and Payment Card Information.

72. Plaintiff and the Classes reasonably assumed the Defendants would comply with basic industry standards for the collection and storage of PII and Payment Card Information.

73. Defendants breached their common law and statutory duties by failing to use reasonable data collection and storage policies and by failing to adequately set up and monitor a secure data storage network. In addition, by storing PII and Payment Card Information on a system vulnerable to unauthorized access, Defendants' negligence continued for at least four years, during which Defendants failed to detect the ongoing breach and failed to upgrade security practices in a way that would end the breach.

74. Because of Defendants' negligence, the PII and Payment Card Information of Plaintiff and the Classes were copied or stolen by unauthorized third parties.

75. Plaintiff and the Classes have been directly and proximately harmed by Defendants' negligence in several ways. Plaintiff and members of the Classes are now at an increased risk of being victims of identity theft and financial impersonation. Plaintiff and members of the Classes will be forced to spend both time and money on monitoring finances, tax records, credit scores, bank accounts, and online accounts to ensure that they have not been victimized.

76. Plaintiff and members of the Classes have suffered, and continue to suffer, injuries including lost time and money in cancelling payment cards, changing or closing accounts, and taking other steps to protect their identities.

77. But for Defendant's negligence, the PII and Payment Card Information of Plaintiff and the Classes would not have been exposed or, in the least, Plaintiff and the Classes would have learned of the breach at an earlier time when the risk and damage would have been mitigated.

SECOND CAUSE OF ACTION
Negligence *Per Se*

78. Plaintiff incorporates by reference all of the above allegations as if fully set forth herein.

79. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses such as Defendants of failing to use reasonable measures to protect PII and Payment Card Information. The FTC publications described above form part of the basis of Defendants' duty.

80. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and Payment Card Information and by not complying with applicable

industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the amount and nature of the PII and Payment Card Information obtained and stored, the length of time the information was maintained on a vulnerable system, and the foreseeable consequences of a data breach, including the damages that would result to consumers.

81. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

82. Plaintiff and members of the Classes are consumers and are within the class of persons that Section 5 of the FTC Act was intended to protect.

83. The harm resulting from Defendants' breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued over 50 enforcement actions against businesses that failed to employ reasonable data security measures and avoid unfair and deceptive practices, causing the same harm suffered by Plaintiff and the Classes.

84. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Classes have suffered, and continue to suffer, injury including lost time and money in cancelling debit and credit cards, changing or closing accounts, and taking other steps to monitor their identities and protect themselves.

THIRD CAUSE OF ACTION Declaratory and Equitable Relief

85. Plaintiff incorporates by reference all of the above allegations as if set forth fully herein.

86. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts which are tortious and which violate the terms of the statutes described herein.

87. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendants continue to owe a legal duty to secure their customers' PII and Payment Card Information;
- b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure their customers' PII and Payment Card Information; and
- c. Defendants' ongoing breaches of their legal duty continue to cause Plaintiff and the Classes harm.

88. The Court should also issue corresponding injunctive relief requiring Defendants to employ security protocols that are consistent with industry standards to protect PII and Payment Card Information. Specifically, this injunction should require Defendants to:

- a. Utilize industry standard encryption to encrypt the transmission of cardholder data at all times;
- b. Implement encryption keys in accordance with industry standards;
- c. Implement EMV technology;
- d. Engage third-party auditors, consistent with industry standards, to test systems for weakness and upgrade any such weakness found;
- e. Audit, test, and train data security personnel regarding any new or modified procedures and how to respond to a data breach;
- f. Regularly test systems for security vulnerabilities, consistent with industry standards;

- g. Comply with all PCI-DSS standards pertaining to the security of customers' PII and Payment Card Information; and
- h. Install all upgrades recommended by manufacturers of security software and firewalls used by Defendants.

89. If an injunction is not issued, Plaintiff and the Classes will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another breach is real, immediate, and substantial. If Defendants' data is breached again, Plaintiff and the members of the Classes will not have an adequate remedy at law because the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct. While monetary damages are warranted for the damages that are legally quantifiable and provable, they are not sufficient to cover the full extent of injuries suffered by Plaintiff and the Classes.

90. The hardship to Plaintiff and the Classes, if an injunction is not issued, exceeds the hardship to Defendants, if an injunction is issued. If another data breach of this scale occurs with Defendants' data, Plaintiff and members of the Classes will likely incur millions of dollars in damages. Conversely, the cost to Defendants of complying with an injunction requiring them to employ reasonable security measures that should have already been in place is relatively minimal.

91. Issuance of the requested injunction will benefit the public by preventing another breach of Defendants' systems, thus eliminating the injuries that would result to Plaintiff, the Classes, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Classes, respectfully requests that the Court:

- A. Certify the Class and Subclass and appoint Plaintiff and Plaintiff's counsel to represent the Classes;
- B. Enter a monetary judgment in favor of Plaintiff and the Classes to compensate them for the injuries they have suffered, together with pre-judgment and post-judgment interest;
- C. Enter a declaratory judgment as described herein;
- D. Grant the injunctive relief requested herein;
- E. Award Plaintiff and the Classes reasonable attorney's fees and costs of suits, as allowed by law; and
- F. Award such other and further relief as this Court may deem just and proper.


DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

DATED: March 26, 2019

Respectfully submitted,

BY: _____


JOSEPH HENRY (HANK) BATES, III (ABN 98063)
TIFFANY WYATT OLDHAM (ABN 2001287)
DAVID SLADE (ABN 2013143)
CARNEY BATES & PULLIAM, PLLC
519 W. 7th St.
Little Rock, AR 72201
Tel: (501) 312-8500
Fax: (501) 312-8505